

Aruba 7XXX Series Controllers

with ArubaOS FIPS Firmware
Non-Proprietary Security Policy
FIPS 140-2 Level 2



a Hewlett Packard
Enterprise company

Version 1.3
February 2020

Copyright

© 2020 Hewlett Packard Enterprise Company. Hewlett Packard Enterprise Company trademarks include  , Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners. Open Source Code

Certain Hewlett Packard Enterprise Company products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.



www.arubanetworks.com

3333 Scott Blvd
Santa Clara, CA 95054
Phone: 408.227.4500
Fax 408.227.4550

Contents

Contents	3
1. Purpose of this Document	5
1.1. Related Documents.....	5
1.1.1. Additional Product Information.....	5
2. Overview	6
2.1. Physical Description	7
2.1.1. Cryptographic Module Boundaries.....	7
2.2. Intended Level of Security	12
3. Physical Security.....	13
4. Operational Environment	13
5. Logical Interfaces	13
6. Roles and Services.....	14
6.1. Crypto Officer Role.....	14
6.2. User Role	18
6.3. Authentication Mechanisms	19
6.4. Unauthenticated Services	21
6.5. Services Available in Non-FIPS Mode.....	21
6.6. Non-Approved Services Disallowed in FIPS Mode	21
7. Cryptographic Key Management	22
7.1. FIPS Approved Algorithms	22
7.2. Non-FIPS Approved but Allowed Cryptographic Algorithms	27
7.3. Non-FIPS Approved Cryptographic Algorithms.....	27
8. Critical Security Parameters.....	28
9. Self-Tests.....	36
9.1. Alternating Bypass State	37
10. Installing the Controller	38
10.1. Pre-Installation Checklist	38
10.2. Precautions	38
10.3. Product Examination.....	38
10.4. Package Contents.....	39

11. Tamper-Evident Labels.....	40
11.1. Reading TELs	40
11.2. Required TEL Locations	41
The Aruba 7010 Mobility Controller requires a minimum of 6 TELs to be applied as follows:.....	43
11.3. Applying TELs	52
11.4. Inspection/Testing of Physical Security Mechanisms	52
12. Ongoing Management	53
12.1. Crypto Officer Management	53
13. User Guidance.....	54
13.1. Setup and Configuration	54
13.2. Setting Up Your Controller	54
13.3. Enabling FIPS Mode.....	54
13.3.1. Enabling FIPS Mode with the CLI	54
13.3.2. Disabling the LCD	55
13.4. Disallowed FIPS Mode Configurations	55
13.5. Full Documentation.....	55

1. Purpose of this Document

This release supplement provides information regarding the Aruba 7XXX Controllers with FIPS 140-2 Level 2 validation from Aruba Networks. The material in this supplement modifies the general Aruba hardware and firmware documentation included with this product and should be kept with your Aruba product documentation.

This supplement primarily covers the non-proprietary Cryptographic Module Security Policy for the Aruba Controller. This security policy describes how the controller meets the security requirements of FIPS 140-2 Level 2 and how to place and maintain the controller in a secure FIPS 140-2 mode. This policy was prepared as part of the FIPS 140-2 Level 2 validation of the product.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) website at:

<http://csrc.nist.gov/groups/STM/cmvp/index.html>

In addition, in this document, the Aruba 7XXX Series Controllers are referred to as the controller, the module, Aruba 7XXX series Mobility Controllers, Aruba 7XXX Controllers, 7XXX Controller, and 7XXX Series.

1.1. Related Documents

The following items are part of the complete installation and operations documentation included with this product:

- *Aruba 7XXX Mobility Controller Installation Guide*
- *Aruba 7XXX-series Mobility Controller Installation Guide*
- *ArubaOS 8.5.0.0 User Guide*
- *ArubaOS 8.5.0.x CLI Reference Guide*
- *ArubaOS 8.5.0.0 Getting Started Guide*
- *ArubaOS 8.5.0.0 Migration Guide*
- *ArubaOS 8.2.2.0 User Guide*
- *ArubaOS 8.2.2.x CLI Reference Guide*
- *ArubaOS 8.2.2.0 Getting Started Guide*
- *ArubaOS 8.2.2.0 Migration Guide*
- *Aruba AP Installation Guides*

1.1.1. Additional Product Information

More information is available from the following sources:

- The Aruba Networks Web-site contains information on the full line of products from Aruba Networks:
<http://www.arubanetworks.com>
- The NIST Validated Modules Web-site contains contact information for answers to technical or sales-related questions for the product:
<http://csrc.nist.gov/groups/STM/cmvp/index.html>

2. Overview

Aruba 7XXX series Mobility Controllers are optimized for 802.11ac and mobile app delivery. Fully application-aware, the 7XXX series prioritizes mobile apps based on user identity and offers exceptional scale for BYOD transactions and device densities.

With a new central processor employing eight CPU cores and four virtual cores, the 7XXX series supports over 32,000 wireless devices and performs stateful firewall policy enforcement at speeds up to 40 Gbps – plenty of capacity for BYOD and 802.11ac devices.

New levels of visibility, delivered by Aruba AppRF on the controller, allow IT to see applications by user, including top web-based applications like Facebook and Box.

The 7XXX series also manages authentication, encryption, VPN connections, IPv4 and IPv6 services, the Aruba Policy Enforcement Firewall™ with AppRF Technology, Aruba Adaptive Radio Management™, and Aruba RFProtect™ spectrum analysis and wireless intrusion protection.

The Aruba controller configurations validated during the cryptographic module testing included:

- Aruba 7005-RWF1 (HPE SKU JW635A)
- Aruba 7005-USF1 (HPE SKU JW636A)
- Aruba 7008-RWF1 (HPE SKU JX931A)
- Aruba 7008-USF1 (HPE SKU JX932A)
- Aruba 7010-RWF1 (HPE SKU JW702A)
- Aruba 7010-USF1 (HPE SKU JW703A)
- Aruba 7024-RWF1 (HPE SKU JW706A)
- Aruba 7024-USF1 (HPE SKU JW707A)
- Aruba 7030-RWF1 (HPE SKU JW710A)
- Aruba 7030-USF1 (HPE SKU JW711A)
- Aruba 7205-RWF1 (HPE SKU JW739A)
- Aruba 7205-USF1 (HPE SKU JW740A)
- Aruba 7210-RWF1 (HPE SKU JW745A)
- Aruba 7210-USF1 (HPE SKU JW746A)
- Aruba 7220-RWF1 (HPE SKU JW753A)
- Aruba 7220-USF1 (HPE SKU JW754A)
- Aruba 7240-RWF1 (HPE SKU JW761A)
- Aruba 7240XM-RWF1 (HPE SKU JW829A)
- Aruba 7240-USF1 (HPE SKU JW762A)
- Aruba 7240XM-USF1 (HPE SKU JW830A)
- FIPS Kit: 4011570-01 (HPE SKU JY894A). Part number for Tamper Evident Labels
- The firmware version validated is ArubaOS 8.5.0.3-FIPS and ArubaOS 8.2.2.5-FIPS

The functionality provided under ArubaOS 8.5 and 8.2 meets the requirements for CMVP testing for FIPS 140-2 and future releases under AOS 8.5 and 8.2 will maintain compliance to the claims made within this document. The CMVP makes no claim as to the correct operation of the module or the security strengths

of the generated keys when ported to an operational environment which is not listed on the validation certificate.

Note: For radio regulatory reasons, part numbers ending with -USF1 are to be sold in the US only. Part numbers ending with -RWF1 are considered 'rest of the world' and must not be used for deployment in the United States. From a FIPS perspective, both -USF1 and -RWF1 models are identical and fully FIPS compliant.

2.1. Physical Description

2.1.1. Cryptographic Module Boundaries

For FIPS 140-2 Level 2 validation, the Controller has been validated as a multi-chip standalone cryptographic module. The opaque hard plastic (Aruba 7005/7008 Controllers only) or metal chassis physically encloses the complete set of hardware and firmware components and represents the cryptographic boundary of the module. The cryptographic boundary is defined as encompassing the top, front, left, right, rear, and bottom surfaces of the chassis.



Figure 1 - The Aruba 7005 controller

Figure 1 shows the front of the Aruba 7005 Controller, and illustrates the following:

- Four Gigabit Ethernet ports
- One Type A USB port
- LINK/ACT and Status LEDs
- Management/Status LED
- Console Connections - RJ-45 and Mini-USB (Disabled in FIPS mode by TELs)



Figure 2 - The Aruba 7008 controller

Figure 2 shows the front of the Aruba 7008 Controller, and illustrates the following:

- Eight Gigabit Ethernet ports with POE
- Two Type A USB ports
- LINK/ACT and Status LEDs
- Management/Status LED
- Console Connections - RJ-45 and Mini-USB (Disabled in FIPS mode by TELs)



Figure 3 - The Aruba 7010 controller

Figure 3 shows the front of the Aruba 7010 Controller, and illustrates the following:

- Sixteen 10/100/1000 Ethernet ports
- Two Small Form-Factor Pluggable (SFP) Uplink ports
- Two Type A USB ports
- LINK/ACT and Status LEDs
- Management/Status LED
- LCD Panel
- Navigation Buttons (Functionally disabled in FIPS mode)
- Console Connections - RJ-45 and Mini-USB (Disabled in FIPS mode by TELs)

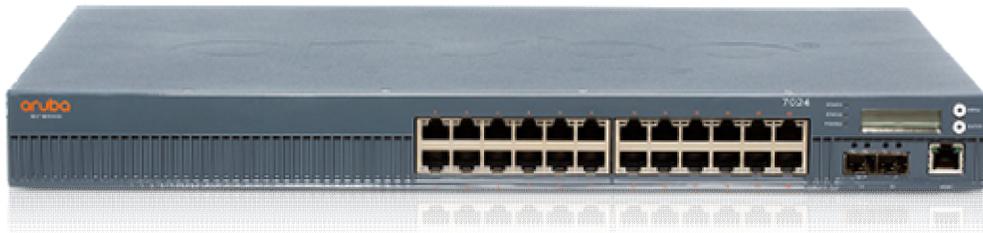


Figure 4 - *The Aruba 7024 controller*

Figure 4 shows the front of the Aruba 7024 Controller, and illustrates the following:

- Twenty-four 10/100/1000 Ethernet ports
- Two Enhanced Small Form-Factor Pluggable (SFP+) Uplink ports
- One Type A USB ports
- LINK/ACT and Status LEDs
- Management/Status LED
- LCD Panel
- Navigation Buttons (Functionally disabled in FIPS mode)
- Console Connections - RJ-45 and Mini-USB (Disabled in FIPS mode by TELs)



Figure 5 - The Aruba 7030 controller chassis

Figure 5 shows the front of the Aruba 7030 Controller, and illustrates the following:

- Eight 10/100/1000 Ethernet ports
- Eight Small Form-Factor Pluggable (SFP) Uplink ports
- One Type A USB port
- LINK/ACT and Status LEDs
- Management/Status LED
- LCD Panel
- Navigation Buttons (Functionally disabled in FIPS mode)
- Console Connections - RJ-45 and Mini-USB (Disabled in FIPS mode by TELs)



Figure 6 - The Aruba 7205 controller chassis

Figure 6 shows the front of the Aruba 7205 Controller, and illustrates the following:

- Four 10/100/1000 Ethernet ports
- Four Small Form-Factor Pluggable (SFP) Uplink ports
- Two Dual-Purpose Gigabit Uplink Ports
- Two Type A USB ports (one is on the front and one is on the back)
- LINK/ACT and Status LEDs
- Management/Status LED
- LCD Panel
- Navigation Buttons (Functionally disabled in FIPS mode)
- Console Connections - RJ-45 and Mini-USB (Disabled in FIPS mode by TELs)



Figure 7 - The Aruba 7200 controller chassis

Figure 7 shows the front of the Aruba 7200 Controller, and illustrates the following:

- Four 10GBase-X (SFP+) Ethernet ports
- Two Dual-Purpose Gigabit Uplink Ports
- LINK/ACT and Status LEDs
- Management/Status LED
- USB 2.0 Port
- LCD Panel and Navigation Buttons (Functionally disabled in FIPS mode)
- Console Connections - RJ-45 and Mini-USB (Disabled in FIPS mode by TELs)
- Expansion Slot (Functionally disabled in FIPS mode).

The Aruba 7210, 7220, and 7240 are identical in terms of outward appearance and definition of the cryptographic boundary. Differences between the models are internal and are related to CPU capacity and speed.

2.2.Intended Level of Security

The 7XXX Controller and associated modules are intended to meet overall FIPS 140-2 Level 2 requirements as shown in Table 1.

Table 1 *Intended Level of Security*

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
Overall	Overall module validation level	2

3. Physical Security

The Aruba Controller is a scalable, multi-processor standalone network device and is enclosed in a robust steel or plastic housing. The enclosure of the module has been designed to satisfy FIPS 140-2 Level 2 physical security requirements.

The Aruba 7XXX Controller requires Tamper-Evident Labels (TEs) to allow the detection of the opening of the chassis cover and to block the Serial console port.

To protect the Aruba 7XXX Controller from any tampering with the product, TEs should be applied by the Crypto Officer as covered under [“Tamper-Evident Labels.”](#)

4. Operational Environment

The operational environment is non-modifiable. The control plane Operating System (OS) is Linux, a real-time, multi-threaded operating system that supports memory protection between processes. Access to the underlying Linux implementation is not provided directly. Only Aruba Networks provided interfaces are used, and the CLI is a restricted command set. The module only allows the loading of trusted and verified firmware that is signed by Aruba. Any firmware loaded into this module that is not shown on the module certificate is out of the scope of this validation and requires a separate FIPS 140-2 validation.

5. Logical Interfaces

All of these physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in the following table.

Table 2 FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	Module Physical Interface
Data Input Interface	<ul style="list-style-type: none">• 10/100/1000 Ethernet Ports• SFP/SFP+ Uplink Ports• USB Port
Data Output Interface	<ul style="list-style-type: none">• 10/100/1000 Ethernet Ports• SFP/SFP+ Uplink Ports• USB Port
Control Input Interface	<ul style="list-style-type: none">• 10/100/1000 Ethernet Ports• SFP/SFP+ Uplink Ports• Reset Switch
Status Output Interface	<ul style="list-style-type: none">• 10/100/1000 Ethernet Ports• SFP/SFP+ Uplink Ports• USB Port• LEDs
Power Interface	<ul style="list-style-type: none">• Power Supply

Data input and output, control input, status output, and power interfaces are defined as follows:

- Data input and output are the packets that use the firewall, VPN, and routing functionality of the modules.
- Control input consists of manual control inputs reset through the reset switch. It also consists of all of the data that is entered into the controller while using the management interfaces.
- Status output consists of the status indicators displayed through the LEDs, the status data that is output from the controller while using the management interfaces, and the log file.
- LEDs indicate the physical state of the module, such as power-up (or rebooting), utilization level, activation state (including fan, ports, and power). The log file records the results of self-tests, configuration errors, and monitoring data.
- A power supply is used to connect the electric power cable.

The controller distinguishes between different forms of data, control, and status traffic over the network ports by analyzing the packets header information and contents.

6. Roles and Services

The Aruba Controller supports role-based authentication. There are two roles in the module (as required by FIPS 140-2 Level 2) that operators may assume: a Crypto Officer role and a User role. The Administrator maps to the Crypto-Officer role and the client Users map to the User role

6.1. Crypto Officer Role

The Crypto Officer role has the ability to configure, manage, and monitor the controller. This role can be present on the controller in a standalone configuration or provided through the Aruba Mobility Master when the controller is operating as a managed device. Crypto Officer Users can be created with predefined roles whose services are a subset of the administrator role. Four management interfaces can be used for this purpose:

- SSHv2 CLI

The Crypto Officer can use the CLI to perform non-security-sensitive and security-sensitive monitoring and configuration. The CLI can be accessed remotely by using the SSHv2 secured management session over the Ethernet ports or locally over the serial port. In FIPS mode, the serial port is disabled.

- Web Interface

The Crypto Officer can use the Web Interface as an alternative to the CLI. The Web Interface provides a highly intuitive, graphical interface for a comprehensive set of controller management tools. The Web Interface can be accessed from a TLS-enabled Web browser using HTTPS (HTTP with Secure Socket Layer) on logical port 4343.

- SNMPv3

The Crypto Officer can also use SNMPv3 to remotely perform non-security-sensitive monitoring and use 'get' and 'getnext' commands.

- Mobility Master

The Crypto Officer can use the Mobility Master interface to configure the controller when operating as a managed device.

See the table below for descriptions of the services available to the Crypto Officer role.

Table 3 *Crypto-Officer Services*

Service	Description	Input	Output	CSP/Algorithm Access (please see table 10 below for details)
SSHv2	Provide authenticated and encrypted remote management sessions while using the CLI	SSHv2 key agreement parameters, SSH inputs, and data	SSHv2 outputs and data	26, 27(read/write/delete)
SNMPv3	Provides ability to query management information	SNMPv3 requests	SNMPv3 responses	33, 34, 35 (read/write/delete)
IKEv1/IKEv2-IPSec	Access the module's IPSec services in order to secure network traffic	IKEv1/IKEv2 inputs and data; IPSec inputs, commands, and data	IKEv1/IKEv2 outputs, status, and data; IPSec outputs, status, and data	1,18 (read) 6,7,8 9,10,11 (read/write/delete) 19, 20, 21, 22, 23, 24 and 25 (read/delete)
Configuring Network Management	Create management Users and set their password and privilege level; configure the SNMP agent	Commands and configuration data	Status of commands and configuration data	1,33, 34 (read) 35 (delete)
Configuring the module	Define synchronization features for module	Commands and configuration data	Status of commands and configuration data	None
Configuring Internet Protocol	Set IP functionality	Commands and configuration data	Status of commands and configuration data	None
Configuring Quality of Service (QoS)	Configure QOS values for module	Commands and configuration data	Status of commands and configuration data	None
Configuring VPN	Configure Public Key Infrastructure (PKI); configure the Internet Key Exchange (IKEv1/IKEv2) Security Protocol; configure the IPSec protocol	Commands and configuration data	Status of commands and configuration data	1,18 (read) 14,15, 16, 17(read) 18, 19, 20, 21, 22, 23, 24 and 25 (delete)
Configuring DHCP	Configure DHCP on module	Commands and configuration data	Status of commands and configuration data	None
Configuring Security	Define security features for module, including Access List, Authentication, Authorization and Accounting (AAA), and firewall functionality	Commands and configuration data	Status of commands and configuration data	12, 13 (read/write/delete) 1 (read)

Table 3 *Crypto-Officer Services*

Manage Certificates	Install, and delete X.509 certificates	Commands and configuration data; Certificates and keys	Status of certificates, commands, and configuration	14, 15, 16,17 (write/delete)
NTP Authentication Service	Configure and connect to NTP server using authentication key	Commands and data	NTP output, status, and data	39 (write/delete)
HTTP over TLS	Secure browser connection over Transport Layer Security acting as a Crypto Officer service (web management interface)	TLS inputs, commands, and data	TLS outputs, status, and data	6,7,8, 28, 29 and 30 (read/write/delete), 4, 5 (read/write) 2, 3 (read)
Openflow Agent	Agent run on device for use with Mobility Master SDN. Leveraged by the SDN for discovering of hosts and networks, configuration of networks, and collection of statistics.	Configuration Data and statistic collection	Status of commands and configuration data	None
Status Function	Cryptographic officer may use CLI “show” commands or view WebUI via TLS to view the controller configuration, routing tables, and active sessions; view health, temperature, memory status, voltage, and packet statistics; review accounting logs, and view physical interface status	Commands and configuration data	Status of commands and configurations	None
IPSec tunnel establishment for RADIUS protection	Provided authenticated/encrypted channel to RADIUS server	IKEv1/IKEv2 inputs and data; IPSec inputs, commands, and data	IKEv1/IKEv2 outputs, status, and data; IPSec outputs, status, and data	12 and 18 (read/write/delete) 19, 20, 21, 22, 23, 24 and 25 (write/delete) 1 (read) 4,5 (read/write), 2.3 (read)
Self-Test	Perform FIPS start-up tests on demand	None	Error messages logged if a failure occurs	None
Configuring Bypass Operation	Configure bypass operation on the module	Commands and configuration data	Status of commands and configuration data	None

Table 3 *Crypto-Officer Services*

Updating Firmware ¹	Updating firmware on the module	Commands and configuration data	Status of commands and configuration data	1, 39 (read)
Configuring Online Certificate Status Protocol (OCSP) Responder	Configuring OCSP responder functionality	OCSP inputs, commands, and data	OCSP outputs, status, and data	26, 27, 28, 29 (read)
Configuring Control Plane Security (CPsec)	Configuring Control Plane Security mode to protect communication with APs using IPsec and issue self signed certificates to APs. Hybrid CPsec allows for the ability to enable or disable independently for each zone and allow zones to contain different configurations. Can interact with hardware and virtual appliances through multizone/mesh when CPsec is enabled.	Commands and configuration data, IKEv1/IKEv2 inputs and data; IPsec inputs, commands, and data	Status of commands, IKEv1/ IKEv2 outputs, status, and data; IPsec outputs, status, and data and configuration data, self signed certificates	12 and 18 (read/write/delete) 19, 20, 21, 22, 23, 24, 25 (write/delete) 1, 2, 3 (read) 4,5 (read/write)
Zeroization	<p>The cryptographic keys stored in SDRAM memory can be zeroized by rebooting the module. The cryptographic keys (IKEv1 Pre-shared key and 802.11i Pre-Shared Key) stored in the flash can be zeroized by using the command 'wipe out flash' or overwriting with a new secret. The 'no' command in the CLI can be used to zeroize IKE, Ipsec and CA CSPs. Please See CLI guide for details. The other keys/CSPs (RSA/ECDSA public key/private key and certificate) stored in Flash memory can be zeroized by using the appropriate command. The "wipe out flash" command formats the configuration flash partition.</p> <p>Additionally, the zeroize TPM command 'zeroize-tpm-keys' may be issued to erase the stored TPM keys.</p> <p>NOTE: The effect of the zeroize TPM command is not reversible. The action will void the warranty on the controller and nullify the</p>	Command	Progress information	All CSPs will be destroyed.

¹ Any firmware loaded into this module that is not shown on the module certificate is out of the scope of this validation and requires a separate FIPS 140-2 validation.

Table 3 *Crypto-Officer Services*

	RMA. The command will wipe the contents of the TPM and render the controller permanently inoperable.			
--	--	--	--	--

6.2. User Role

Table 4 below lists the services available to User role:

Table 4 <i>User Service</i>				
Service	Description	Input	Output	CSP Access (please see table 10 below for CSP details)
IKEv1/IKEv2-IPSec	Access the module's IPSec services in order to secure network traffic	IPSec inputs, commands, and data	IPSec outputs, status, and data	6,7,8, 9,10,11 (read, write, delete) 14,15,16,17 (read) 19, 20, 21, 22, 23, 24 and 25 (read/delete) 4,5 (read/write), 2.3 (read)
HTTP over TLS	Access the module's TLS services in order to secure network traffic	TLS inputs, commands, and data	TLS outputs, status, and data	6,7, 8, 9, 10, 11, 28, 29, 31 (read/write/delete) 4,5 (read/write), 2.3 (read)
802.11i Shared Key Mode	Access the module's 802.11i services in order to secure network traffic	802.11i inputs, commands and data	802.11i outputs, status and data	33, 34, 35 and 36 (create/read/delete) 4,5 (read/write)
802.11i with EAP-TLS	Access the module's 802.11i services in order to secure network traffic	802.11i inputs, commands and data	802.11i outputs, status, and data	14,15,16,17 (read) 34, 35, 36 and 37 (read/delete) 4,5 (read/write)

6.3. Authentication Mechanisms

The Aruba Controller supports role-based authentication. Role-based authentication is performed before the Crypto Officer enters privileged mode using admin password via Web Interface or SSHv2. Role-based authentication is also performed for User authentication.

This includes password and RSA/ECDSA-based authentication mechanisms. The strength of each authentication mechanism is described below.

Table 5 Estimated Strength of Authentication Mechanisms

Authentication Type	Role	Strength
Password-based authentication (SSH and Web Interface)	Crypto Officer	<p>Passwords are required to be a minimum of eight ASCII characters and a maximum of 32 with a minimum of one letter and one number. Given these restrictions, the probability of randomly guessing the correct sequence is one (1) in 3,608,347,333,959,680 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. The calculation should be 94^8 (Total number of 8-digit passwords) – 84^8 (Total number of 8-digit passwords without numbers) – 42^8 (Total number of 8-digit passwords without letters) + 32^8 (Total number of 8-digit passwords without letters or numbers, added since it is double-counted in the previous two subtractions) = 3,608,347,333,959,680). At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is $60,000/3,608,347,333,959,680$, which is less than 1 in 100,000 required by FIPS 140-2</p>
RSA-based authentication (IKEv1/IKEv2/TLS/EAP-TLS)	User	<p>The module supports 2048-bit RSA key authentication during IKEv1, IKEv2, TLS, and EAP-TLS. RSA 2048 bit keys correspond to 112 bits of security. Assuming the low end of that range, the associated probability of a successful random attempt is 1 in 2^{112}, which is less than 1 in 1,000,000 required by FIPS 140-2. At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is $60,000/2^{112}$, which is less than 1 in 100,000 required by FIPS 140-2.</p>
RSA-based authentication (SSH/HTTP over TLS)	Crypto Officer	<p>The module supports 2048-bit RSA key authentication during IKEv1, IKEv2, TLS, and EAP-TLS. RSA 2048 bit keys correspond to 112 bits of security. Assuming the low end of that range, the associated probability of a successful random attempt is 1 in 2^{112}, which is less than 1 in 1,000,000 required by FIPS 140-2. At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is $60,000/2^{112}$, which is less than 1 in 100,000 required by FIPS 140-2.</p> <p>These keys can be used for admin authentication.</p>

ECDSA-based authentication (IKEv1/IKEv2/TLS/EAP-TLS)	User	ECDSA signing and verification is used to authenticate to the module during IKEv1/IKEv2, TLS, and EAP-TLS. Both P-256 and P-384 curves are supported. ECDSA P-256 provides 128 bits of equivalent security, and P-384 provides 192 bits of equivalent security. Assuming the low end of that range, the associated probability of a successful random attempt during a one-minute period is 1 in 2^{128} , which is less than 1 in 1,000,000 required by FIPS 140-2. At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is $60,000/2^{128}$, which is less than 1 in 100,000 required by FIPS 140-2.
ECDSA-based authentication (SSH/HTTP over TLS)	Crypto Officer	ECDSA signing and verification is used to authenticate to the module during IKEv1/IKEv2, TLS, and EAP-TLS. Both P-256 and P-384 curves are supported. ECDSA P-256 provides 128 bits of equivalent security, and P-384 provides 192 bits of equivalent security. Assuming the low end of that range, the associated probability of a successful random attempt during a one-minute period is 1 in 2^{128} , which is less than 1 in 1,000,000 required by FIPS 140-2. At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is $60,000/2^{128}$, which is less than 1 in 100,000 required by FIPS 140-2. These keys can be used for admin authentication.
Pre-shared key-based authentication (RADIUS)	User	The password requirements are the same as the CO role above, except that the maximum ASCII characters can be 128. Assuming the weakest option of 8 ASCII characters, the authentication mechanism strength is the same as the CO role above.
Pre-shared key-based authentication (IKEv1/IKEv2)	User	The password requirements are the same as the CO role above, except that the maximum ASCII characters can be 64. Additionally, exactly 64 HEX characters can be entered. Assuming the weakest option of 8 ASCII characters, the authentication mechanism strength is the same as the CO role above.
Pre-shared key based authentication (802.11i)	User	The password requirements are the same as the IKEv1/IKEv2 shared secret above, except that the maximum ASCII characters can be 63. Assuming the weakest option of 8 ASCII characters, the authentication mechanism strength is the same as the IKEv1/IKEv2 shared secret above.
SSH Master Public Certificate (SSH)	Crypto Officer	RSA-based certificate used for authentication by the CO to connect to the Mobility Master which provides interface to the controller if running as a managed device. Same authentication mechanism strength as RSA-based authentication above.

6.4.Unauthenticated Services

The Aruba Controller can perform VLAN, bridging, firewall, routing, and forwarding functionality without authentication. These services do not involve any cryptographic processing.

- Internet Control Message Protocol (ICMP) service
- Network Time Protocol (NTP) service
- Network Address Resolution Protocol (ARP) service

Additional unauthenticated services include performance of the power-on self-test and system status indication via LEDs.

6.5.Services Available in Non-FIPS Mode

- All of the services that are available in FIPS mode are also available in non-FIPS mode.
- If not operating in the Approved mode as per the procedures in sections 13.1, 13.2 and 13.3, then non-Approved algorithms and/or sizes are available.
- Upgrading the firmware via the console port.
- Debugging via the console port.

6.6.Non-Approved Services Disallowed in FIPS Mode

- WPA3
- WPA-2 Multiple Pre-Shared Key (MPSK), where every client connected to the WLAN SSID may have its own unique PSK.
- IPSec/IKE using Triple-DES

7. Cryptographic Key Management

7.1.FIPS Approved Algorithms

The firmware in each module contains the following cryptographic algorithm implementations/crypto libraries to implement the different FIPS approved cryptographic algorithms that will be used for the corresponding security services supported by the module in FIPS mode:

- ArubaOS OpenSSL library algorithm implementation
- ArubaOS Crypto library algorithm implementation
- ArubaOS UBOOT Bootloader library algorithm implementation
- Aruba Hardware Crypto Accelerator algorithm implementation

Below are the detailed lists for the FIPS approved algorithms and the associated certificate implemented by each algorithm implementation.

Note that not all algorithm modes that appear on the module's CAVP certificates are utilized by the module, and the tables below list only the algorithm modes that are utilized by the module.

Table 6 Hardware CAVP Certificates

Aruba Hardware Crypto Accelerators (Broadcom XLP CPU)					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
2477, 2479 & 3014	AES	FIPS 197, SP 800-38A SP 800-38D	ECB, CBC, CFB8, CFB128, OFB, CTR (ext only) CCM, AES-GCM	128, 192, 256	Data Encryption/Decryption
1520, 1522 & 1906	HMAC	FIPS 198-1	HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	112, 126, 160, 256	Message Authentication
2096, 2098 & 2522	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512 Byte Only		Message Digest
1516, 1518 & 1770	Triple-DES	SP 800-67	TEBC, TCBC	192	Data Encryption/Decryption
1266, 1268 & 1573	RSA	FIPS 186-4	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	2048	Digital Signature Generation and Verification

NOTE: In FIPS Mode, Triple-DES is only used in the Self-Tests.

The above hardware algorithm certificates were tested on Broadcom XLP series processors by Broadcom Corporation. Aruba Networks purchased the processors and put them in the Aruba modules to support bulk cryptographic operations. Please be aware that there is no partnership between Aruba Networks and Broadcom Corporation.

Table 7 ArubaOS OpenSSL CAVP Certificates

ArubaOS OpenSSL					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
2900	AES	FIPS 197, SP 800-38A	ECB, CBC, CFB (128only), CTR (ext only)	128, 192, 256	Data Encryption/Decryption
C81, C82, C83	AES	FIPS 197, SP 800-38A SP 800-38D	GCM, CCM (used in self-tests only)	128, 192, 256	Data Encryption/Decryption
326	CVL IKEv1, TLS, SSH, SNMP	SP800-135	IKEv1: DSA, PSK TLS: v1.0/1.1, v1.2	IKEv1: DH 2048-bit; SHA-1, SHA-256, SHA-384 SSH: SHA-1 TLS: SHA-256, SHA-384, SHA-512	Key Derivation
528	DRBG	SP 800-90A	AES CTR	256	Deterministic Random Number Generation
1598	ECDSA	186-4		P256, P384	Digital Key Generation, Signature Generation and Verification
1835	HMAC	FIPS 198-1	HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	112, 126, 160, 256	Message Authentication
32	KBKDF	SP 800-108	CTR	HMAC-SHA1, HMAC-SHA256, HMAC-	Deriving Keys

				SHA384	
1528	RSA	FIPS 186-2	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	1024 (legacy SigVer only), 2048	Digital Signature Verification
1528	RSA	FIPS 186-4	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	2048	Digital Key Generation, Signature Generation and Verification
2440	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512 Byte Only		Message Digest
1510	DSA	FIPS 186-4		2048	Key Generation, PQG Generation
1726	Triple-DES	SP 800-67	TEBC, TCBC	192	Data Encryption/Decryption
AES 2900 HMAC 1835	KTS	SP 800-38F	AES-CBC ²	128, 192, 256	Key Wrapping/Key Transport via IKE/IPSec

Note:

- In FIPS Mode, Triple-DES is only used in the Self-Tests and with the KEK.
- RSA (Cert. #1528; non-compliant with the functions from the CAVP Historical RSA List)
 - ❖ FIPS186-2:
 - ALG[ANSIX9.31]: Key(gen)(MOD: 1024 PubKey Values: 65537)
 - ALG[RSASSA-PKCS1_V1_5]: SIG(gen): 1024, SHS: SHA-1/SHA-256/SHA-384/SHA-512, 2048, SHS: SHA-1
- ECDSA (Cert. #524; non-compliant with the functions from the CAVP Historical ECDSA List)
 - ❖ FIPS186-2:
 - SIG(gen): CURVES(P-256 P-384), SHS: SHA-1

² key establishment methodology provides between 128 and 256 bits of encryption strength

Table 8 ArubaOS Crypto Module CAVP Certificates

ArubaOS Crypto Module					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
2884	AES	FIPS 197, SP 800-38A SP 800-38D	CBC, CTR, GCM	128, 192, 256	Data Encryption/Decryption
314	CVL IKEv1 (KDF) IKEv2 (KDF)	SP800-135	IKEv1: DSA, PSK	IKEv1: DH 256, 384, 2048-bit; SHA-256, SHA-384 IKEv2: DH 2048-bit; SHA-256, SHA-384	Key Derivation
1288, 1289, 1290	DSA	FIPS 186-4		2048	Key Generation, PQG Generation
519	ECDSA	186-4		P256, P384	Digital Key Generation, Signature Generation and Verification
1206, 1207, 1208	ECDSA	186-4		P256, P384	Key Verification
1818	HMAC	FIPS 198-1	HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 HMAC-SHA-1-96, HMAC-SHA-256-128, HMAC-SHA-384-192	112, 126, 160, 256 112, 126, 160	Message Authentication
1518	RSA	FIPS 186-2	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	1024 (legacy SigVer only), 2048	Digital Signature Verification
1518	RSA	FIPS 186-4	SHA-1, SHA-256, SHA-384, SHA-512	2048	Digital Key Generation, Signature Generation and

			PKCS1 v1.5		Verification
2425	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512 Byte Only		Message Digest
1720	Triple-DES	SP 800-67	TCBC	192	Data Encryption/Decryption
AES 2884	KTS	SP 800-38F	AES-GCM ³	128, 192, 256	Key Wrapping/Key Transport via IKE/IPSec
AES 2884 HMAC 1818	KTS	SP 800-38F	AES-CBC ⁴	128, 192, 256	Key Wrapping/Key Transport via IKE/IPSec

Note:

- In FIPS Mode, Triple-DES is only used in the Self-Tests.
- RSA (Cert. #1518; non-compliant with the functions from the CAVP Historical RSA List)
 - ❖ FIPS186-2:
 - ALG[ANSIX9.31]: Key(gen)(MOD: 1024 PubKey Values: 65537)
 - ALG[RSASSA-PKCS1_V1_5]: SIG(gen): 1024, SHS: SHA-1/SHA-256/SHA-384/SHA-512, 2048, SHS: SHA-1
- ECDSA (Cert. #519; non-compliant with the functions from the CAVP Historical ECDSA List)
 - ❖ FIPS186-2:
 - SIG(gen): CURVES(P-256 P-384), SHS: SHA-1

³ key establishment methodology provides between 128 and 256 bits of encryption strength

⁴ key establishment methodology provides between 128 and 256 bits of encryption strength

Table 9 ArubaOS UBOOT Bootloader CAVP Certificates

ArubaOS UBOOT Bootloader					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
2394	RSA	FIPS 186-4	SHA-1, SHA-256	2048	Digital Signature Verification
3631	SHS	FIPS 180-4	SHA-1, SHA-256 Byte Only		Message Digest

NOTE: Only Firmware signed with SHA-256 is permitted in the Approved mode. Digital signature verification with SHA-1, while available within the module, shall only be used while in the non-Approved mode.

7.2. Non-FIPS Approved but Allowed Cryptographic Algorithms

- MD5 (used for older versions of TLS)
- NDRNG (used solely to seed the approved DRBG)
- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
- EC Diffie-Hellman (key agreement; key establishment methodology provides 128 or 192 bits of encryption strength)

Note: RSA key wrapping is used in TLS protocol implementation.

7.3. Non-FIPS Approved Cryptographic Algorithms

The cryptographic module implements the following non-approved algorithms that are not permitted for use in the FIPS 140-2 mode of operations:

- DES
- HMAC-MD5
- MD5
- RC4
- RSA (non-compliant less than 112 bits of encryption strength)
- Null Encryption
- Diffie-Hellman (key agreement; non-compliant less than 112 bits of encryption strength)
- EC Diffie-Hellman (key agreement; non-compliant less than 112 bits of encryption strength)
- Triple-DES as used in IKE/IPSec
- Diffie-Hellman Group14 with SHA-256

These algorithms are used for older version of TLS, SSH and WEP in non-FIPS mode.

NOTE: IKEv1, IKEv2, TLS, SSH and SNMP protocols have not been reviewed or tested by the CAVP and CMVP.

8. Critical Security Parameters

The following are the Critical Security Parameters (CSPs) used in the module. The user is responsible for zeroizing all CSPs when switching modes.

Table 10 CSPs/Keys Used in the module

#	Name	Algorithm/Key Size	Generation/Use	Storage	Zeroization
General Keys/CSPs					
1	Key Encryption Key (KEK) – Not Considered as a CSP	Triple-DES (192 bits)	Hardcoded during manufacturing. This is used to obfuscate keys.	Stored in Flash memory (plaintext).	The zeroization requirements do not apply to this key as it is not considered a CSP.
2	DRBG entropy input	SP800-90a CTR_DRBG (512 bits)	Entropy inputs to the DRBG function used to construct the DRBG seed. 64 bytes are gotten from the entropy source on each call by any service that requires a random number.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
3	DRBG seed	SP800-90a CTR_DRBG (384-bits)	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from the entropy source, by any service that requires a random number	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
4	DRBG Key	SP800-90a CTR_DRBG (256 bits)	This is the DRBG key used for SP800-90a CTR_DRBG.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
5	DRBG V	SP800-90a CTR_DRBG V (128 bits)	Internal V value used as part of SP800-90a CTR_DRBG	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
6	Diffie-Hellman private key	Diffie-Hellman Group 14 (224 bits)	Generated internally by calling FIPS approved DRBG (cert #528) during Diffie-Hellman Exchange. Used for establishing DH shared	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module

Table 10 CSPs/Keys Used in the module

			secret.		
7	Diffie-Hellman public key	Diffie-Hellman Group 14 (2048 bits)	Generated internally by calling FIPS approved DRBG (cert #528) during Diffie-Hellman Exchange. Used for establishing DH shared secret.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
8	Diffie-Hellman shared secret	Diffie-Hellman Group 14 (2048 bits)	Established during Diffie-Hellman Exchange. Used for deriving IPSec/IKE and SSH cryptographic keys.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
9	EC Diffie-Hellman private key	EC Diffie-Hellman (Curves: P-256 or P-384).	Generated internally by calling FIPS approved DRBG (cert #528) during EC Diffie-Hellman Exchange. Used for establishing ECDH shared secret.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
10	EC Diffie-Hellman public key	EC Diffie-Hellman (Curves: P-256 or P-384).	Generated internally by calling FIPS approved DRBG (cert #528) during EC Diffie-Hellman Exchange. Used for establishing ECDH shared secret.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
11	EC Diffie-Hellman shared secret	EC Diffie-Hellman (Curves: P-256 or P-384)	Established during EC Diffie-Hellman Exchange. Used for deriving IPSec/IKE and TLS cryptographic keys.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
12	RADIUS server shared secret	8-128 characters shared secret	Entered by CO role. Used for RADIUS server authentication.	Stored in Flash memory obfuscated with KEK.	Zeroized by using command 'wipe out flash' or by overwriting with a new secret
13	Crypto Officer Password	8-32 characters password	Entered by CO role. Used for CO role authentication.	Stored in Flash memory obfuscated with KEK	Zeroized by using command 'wipe out flash' or by overwriting with a new secret

Table 10 CSPs/Keys Used in the module

14	RSA Private Key	RSA 2048 bit private key	This key is generated by calling FIPS approved DRBG (cert #528) in the module. Used for IKEv1, IKEv2, TLS, OCSP (signing OCSP messages) and EAP-TLS peers authentication. This key can also be entered by the CO	Stored in Flash memory obfuscated with KEK.	Zeroized by using command 'wipe out flash'
15	RSA public key	RSA 2048 bits public key	This key is generated by calling FIPS approved DRBG (cert #528) in the module. This key can also be entered by the CO Used for IKEv1, IKEv2, TLS, OCSP (verifying OCSP messages) and EAP-TLS peers authentication.	Stored in Flash memory obfuscated with KEK.	Zeroized by using command 'wipe out flash'
16	ECDSA Private Key	ECDSA suite B P-256 and P-384 curves	This key is generated by calling FIPS approved DRBG (cert #528) in the module. Used for IKEv1, IKEv2, TLS and EAP-TLS peers authentication. This key can also be entered by the CO	Stored in Flash memory obfuscated with KEK.	Zeroized by using command 'wipe out flash'
17	ECDSA Public Key	ECDSA suite B P-256 and P-384 curves	This key is generated by calling FIPS approved DRBG (cert #528) in the module. This key can also be entered by the CO Used for IKEv1, IKEv2, TLS and EAP-TLS peers authentication.	Stored in Flash memory obfuscated with KEK.	Zeroized by using command 'wipe out flash'
IPSec/IKE					
18	IKEv1 Pre-shared secret	Shared secret (8 - 64 ASCII or 64 HEX characters)	Entered by CO role. Used for IKEv1 peers authentication.	Stored in Flash memory obfuscated with KEK.	Zeroized by using command 'wipe out flash' or by overwriting with a new secret

Table 10 CSPs/Keys Used in the module

19	skeyid	Shared Secret (160/256/384 bits)	A shared secret known only to IKE peers. It was established via key derivation function defined in SP800-135 KDF (IKEv1). Used for deriving other keys in IKE protocol implementation.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.
20	skeyid_d	Shared Secret (160/256/384 bits)	A shared secret known only to IKE peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv1). Used for deriving IKE session authentication key.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
21	SKEYSEED	Shared Secret (160/256/384 bits)	A shared secret known only to IKE peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv2) and it will be used for deriving IKE session authentication key.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
22	IKE session authentication key	HMAC-SHA-1/256/384 (160/256/384 bits)	The IKE session (IKE Phase I) authentication key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv1/IKEv2). Used for IKEv1/IKEv2 payload integrity verification.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
23	IKE session encryption key	AES (128/192/256 bits, CBC)	The IKE session (IKE Phase I) encrypt key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv1/IKEv2). Used for IKE payload protection.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module

Table 10 CSPs/Keys Used in the module

24	IPSec session encryption key	AES and AES-GCM (128/192/256 bits, CBC)	The IPsec (IKE phase II) encryption key. This key is derived via a key derivation function defined in SP800-135 KDF (IKEv1/IKEv2). Used for IPSec traffics protection.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
25	IPSec session authentication key	HMAC-SHA-1 (160 bits)	The IPsec (IKE Phase II) authentication key. This key is derived via using the KDF defined in SP800-135 KDF (IKEv1/IKEv2). Used for IPSec traffics integrity verification.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
SSHv2					
26	SSHv2 session key	AES (128/192/256 bits) CBC Mode, CTR Mode	This key is derived via a key derivation function defined in SP800-135 KDF (SSHv2). Used for SSHv2 traffics protection.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
27	SSHv2 session authentication key	HMAC-SHA-1, HMAC-SHA1-96 (160-bit)	This key is derived via a key derivation function defined in SP800-135 KDF (SSHv2). Used for SSHv2 traffics integrity verification.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
TLS					
28	TLS pre-master secret	48 bytes secret	This key is transferred into the module, protected by TLS RSA public key.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
39	TLS session encryption key	AES (128/192/256 bits) CBC Mode, Triple-DES Mode, GCM Mode	This key is derived via a key derivation function defined in SP800-135 KDF (TLS). Used for TLS traffics protection. Uses Triple-DES when	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module

Table 10 CSPs/Keys Used in the module

			using TLSv1.0		
30	TLS session authentication key	HMAC-SHA-1/256/384 (160/256/384 bits)	This key is derived via a key derivation function defined in SP800-135 KDF (TLS). Used for TLS traffic integrity verification.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
SNMPv3					
31	SNMPv3 authentication password	8-31 characters password	Entered by CO role. User for SNMPv3 authentication.	Stored in Flash memory obfuscated with KEK.	Zeroized by using command 'wipe out flash' or by overwriting with a new secret
32	SNMPv3 Authentication Key	AES-CFB key (128 bits)	This key is derived via a key derivation function defined in SP800-135 KDF (SNMPv3). Used for SNMPv3 authentication.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
33	SNMPv3 engine ID	10 – 24 hex character password	Entered by CO role. A unique string used to identify the SNMP engine.	Stored in Flash memory obfuscated with KEK.	Zeroized by using command 'wipe out flash' or by overwriting with a new secret
34	SNMPv3 privacy key	AES-CFB key (128 bits)	This key is derived via a key derivation function defined in SP800-135 KDF (SNMPv3). Used for SNMPv3 traffics protection.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
35	SNMPv3 Privacy Protocol Password	8 - 31 characters password	Entered by CO role. A unique string used to protect SNMP privacy protocol.	Stored in Flash memory (ciphertext) obfuscated with KEK.	Zeroized by using command 'wipe out flash' or by overwriting with a new secret
802.11i					

Table 10 CSPs/Keys Used in the module

36	802.11i Pre-shared secret	Shared secret (8-63 ASCII or 64 HEX characters)	Entered by CO role. Used for 802.11i client/server authentication	Stored in Flash memory obfuscated with KEK.	Zeroized by using command 'wipe out flash' or by overwriting with a new secret
37	802.11i Pair-Wise Master key (PMK)	Shared secret (256 bits)	The PMK is transferred to the module, protected by IPsec secure tunnel. Used to derive the Pairwise Transient Key (PTK) for 802.11i communications.	Stored in SDRAM (plaintext).	Zeroized by rebooting the module
38	802.11i Pairwise Transient Key (PTK)	HMAC (384 bits)	This key is used to derive 802.11i session key by using the KDF defined in SP800-108.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
39	802.11i session key	AES-CCM (128 bits)	Derived during 802.11i 4-way handshake by using the KDF defined in SP800-108 then used as the session key.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module
Factory Key					
40	Factory CA Public Key	RSA (2048 bits)	This is RSA public key. Loaded into the module during manufacturing. Used for Firmware verification.	Stored in TPM	Zeroized by using command 'zeroize-tpm-keys'
NTP					
41	NTP Authentication Key	SHA-1 (160-bit)	Entered by CO role. A unique string used for authentication to the NTP server.	Stored in Flash memory (ciphertext) obfuscated with KEK.	Zeroized by using command 'wipe out flash' or by deleting the NTP configuration.
Mobility Master					
42	Master Public Certificate	RSA (2048 bits)	This key is generated by calling FIPS approved DRBG (cert	Stored in Flash memory (ciphertext) obfuscated with KEK.	Zeroized by using command 'wipe out flash'

Table 10 CSPs/Keys Used in the module

			<p>#528) in the module.</p> <p>Used for SSH to the Mobility Master when connecting to the controllers for management.</p>		
--	--	--	---	--	--

- AES GCM IV generation is performed in compliance with the Implementation Guidance A.5 scenario 1. FIPS approved DRBG (Cert. #528) is used for IV generation and 96 bits of IV is supported.
- For keys identified as being “Generated internally by calling FIPS approved DRBG”, the generated seed used in the asymmetric key generation is an unmodified output from the DRBG.
- Aruba believes the module generates a minimum of 256 bits of entropy for use in key generation through two primary entropy noise sources. The min-entropy rates claimed by the entropy noise source vendors are 70% and 75%. Testing with the NIST SP800-90B test suite of raw data samples from one of the noise sources resulted in significantly better min-entropy than claimed by its vendor, but due to lack of access to unconditioned entropy samples from the other entropy noise source at the time of the evaluation, Aruba has included the following entropy caveat.

The module generates cryptographic keys whose strengths are modified by available entropy.

- CSPs labeled as “Entered by CO” are entered into the module via SSH/TLS.

9. Self-Tests

The module performs Power On Self-Tests regardless the modes (non-FIPS mode and FIPS mode). In addition, the module also performs Conditional tests after being configured into the FIPS mode. In the event any self-test fails, the module will enter an error state, log the error, and reboot automatically.

The module performs the following POSTs (Power On Self-Tests):

- ArubaOS OpenSSL library (Firmware)
 - AES encrypt KAT
 - AES decrypt KAT
 - AES-CCM Encrypt KAT
 - AES-CCM Decrypt KAT
 - AES-GCM Encrypt KAT
 - AES-GCM Decrypt KAT
 - Triple-DES encrypt KAT
 - Triple-DES decrypt KAT
 - DRBG KAT
 - RSA sign KAT
 - RSA verify KAT
 - ECDSA sign KAT
 - ECDSA verify KAT
 - ECDH (P-256) KAT
 - DH (2048) KAT
 - KDF108 KAT
 - DSA Sign KAT
 - DSA Verify KAT
 - SHS (SHA1, SHA256, SHA384 and SHA512) KATs
 - HMAC (HMAC-SHA1, HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512) KATs
- ArubaOS Crypto library (Firmware)
 - AES encrypt KAT
 - AES decrypt KAT
 - AES-CCM encrypt KAT
 - AES-CCM decrypt KAT
 - AES-GCM encrypt KAT
 - AES-GCM decrypt KAT
 - Triple-DES encrypt KAT
 - Triple-DES decrypt KAT
 - DSA Sign KAT
 - DSA Verify KAT
 - SHA (SHA1, SHA256, SHA384 and SHA512) KATs
 - DH (2048) Pairwise Consistency Test
 - ECDH (P-256, P-384) Pairwise Consistency Test
 - HMAC (HMAC-SHA1, HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512) KATs
 - RSA sign KAT
 - RSA verify KAT
 - ECDSA sign KAT
 - ECDSA verify KAT

- ArubaOS UBOOT Bootloader library (Firmware)
 - Firmware Integrity Test: RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256
- Aruba Hardware Crypto Accelerator (Hardware):
 - AES encrypt KAT
 - AES decrypt KAT
 - AES-CCM encrypt KAT
 - AES-CCM decrypt KAT
 - AES-GCM encrypt KAT
 - AES-GCM decrypt KAT
 - Triple-DES encrypt KAT
 - Triple-DES decrypt KAT
 - HMAC (HMAC-SHA1, HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512) KATs
 - RSA sign KAT
 - RSA verify KAT

The module performs the following Conditional Tests:

- ArubaOS OpenSSL library (Firmware)
 - Bypass Tests (Wired Bypass Test and Wireless Bypass Test)
 - CRNG Test on Approved DRBG
 - SP800-90A Section 11.3 Health Tests for DRBG (Instantiate, Generate and Reseed).
 - ECDSA Pairwise Consistency Test
 - RSA Pairwise Consistency Test
 - Firmware Load Test - RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256
 - CRNG Test for NDRNG
- ArubaOS Crypto library (Firmware)
 - RSA Pairwise Consistency Test
 - ECDSA Pairwise Consistency Test
- ArubaOS UBOOT BootLoader library (Firmware)
 - Firmware Load Test - RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256

Self-test results are logged in a log file. Upon successful completion of the power-up self tests, the module logs a KATS: passed message into a log file. Confirm the file update by checking the associated time of the file.

9.1. Alternating Bypass State

The controller implements an alternating bypass state when:

- a port is configured in trusted mode to provide unauthenticated services
- a configuration provides wireless access without encryption

The alternating bypass status can be identified by retrieving the port configuration or the wireless network configuration.

10. Installing the Controller

This chapter covers the physical installation of the 7XXX Controllers with FIPS 140-2 Level 2 validation. The Crypto Officer is responsible for ensuring that the following procedures are used to place the controller in a FIPS-approved mode of operation.

This chapter covers the following installation topics:

- Precautions to be observed during installation
- Requirements for the controller components and rack mounting gear
- Selecting a proper environment for the controller
- Mounting the controller in a rack
- Connecting power to the controller

10.1. Pre-Installation Checklist

You will need the following during installation:

- Aruba 7XXXController components.
- Phillips or cross-head screwdriver.
- Equipment rack.
- Aruba power cord for each power supply, rated to at least 10 A with IEC320 connector.
- Adequate power supplies and electrical power.
- Cool, non-condensing air 0 to 40 °C (32 to 104 °F). May require air conditioning.
- Management Station (PC) with 10/100 Mbps Ethernet port and SSHv2 software.
- A 4- or 8-conductor Category 5 UTP Ethernet cable.

10.2. Precautions

- Installation should be performed only by a trained technician.
- Dangerous voltage in excess of 240 VAC is always present while the Aruba power supply is plugged into an electrical outlet. Remove all rings, jewelry, and other potentially conductive material before working with this product.
- Never insert foreign objects into the chassis, the power supply, or any other component, even when the power supplies have been turned off, unplugged, or removed.
- Main power is fully disconnected from the controller only by unplugging all power cords from their power outlets. For safety reasons, make sure the power outlets and plugs are within easy reach of the operator.
- Do not handle electrical cables that are not insulated. This includes any network cables.
- Keep water and other fluids away from the product.
- Comply with electrical grounding standards during all phases of installation and operation of the product. Do not allow the controller chassis, network ports, power supplies, or mounting brackets to contact any device, cable, object, or person attached to a different electrical ground. Also, never connect the device to external storm grounding sources.
- Installation or removal of the chassis or any module must be performed in a static-free environment. The proper use of anti-static body straps and mats is strongly recommended.
- Keep modules in anti-static packaging when not installed in the chassis.
- Do not ship or store this product near strong electromagnetic, electrostatic, magnetic or radioactive fields.
- Do not disassemble chassis or modules. They have no internal user-serviceable parts. When service or repair is needed, contact Aruba Networks.

10.3. Product Examination

The units are shipped to the Crypto Officer in factory-sealed boxes using trusted commercial carrier shipping companies. The Crypto Officer should examine the carton for evidence of tampering. Tamper-evidence includes tears, scratches, and other irregularities in the packaging.

10.4. Package Contents

The product carton should include the following:

- 7XXX Controller
- Rack mounting kit (optional)
- Aruba User Documentation CD
- Tamper-Evident Labels

11. Tamper-Evident Labels

After testing, the Crypto Officer must apply Tamper-Evident Labels (TELs) to the controller. When applied properly, the TELs allow the Crypto Officer to detect the opening of the chassis cover, the removal or replacement of modules or cover plates, or physical access to restricted ports. Vendor provides **FIPS 140** designated TELs which have met the physical security testing requirements for tamper evident labels under the FIPS 140-2 Standard. TELs are not endorsed by the Cryptographic Module Validation Program (CMVP).



The tamper-evident labels shall be installed for the module to operate in a FIPS Approved mode of operation.



Aruba Provides double the required amount of TELs. If a customer requires replacement TELs, please call customer support and Aruba will provide the TELs (Part # 4011570-01 - HPE SKU JY894A).



The Crypto officer shall be responsible for keeping the extra TELs at a safe location and managing the use of the TELs.

11.1. Reading TELs

Once applied, the TELs included with the controller cannot be surreptitiously broken, removed, or reapplied without an obvious change in appearance:



Figure 8 *Tamper-Evident Labels*

Each TEL also has a unique serial number to prevent replacement with similar labels.

11.2. Required TEL Locations

The Aruba 7005 Mobility Controller requires a minimum of 4 TELs to be applied as follows:

To Detect Opening the Chassis Lid

- Spanning the front left side and right rear corners of the chassis lid where it meets the chassis bottom, as shown in Figures 9 and 10 (Labels 1 & 2).

To Detect Access to Restricted Ports

- Two labels spanning the RJ-45 and mini-USB serial ports, as shown in figure 10. Press down on this label to ensure that it adheres to a sufficient area of the front bezel. The RJ-45 port is raised relative to the bezel so there will be some air gap under the label in this area. However, the air gap should not be larger than 2-3mm.



Figure 9 Required TELs for the Aruba 7005 Mobility Controller – Bottom



Figure 10 Required TELs for the Aruba 7005 Mobility Controller – Front

The Aruba 7008 Mobility Controller requires a minimum of 8 TELs to be applied as follows:

To Detect Opening the Chassis Lid

- Spanning the front left side and right rear corners of the chassis lid where it meets the chassis bottom, as shown in Figures 11 and 12 (Labels 1 & 2).

To Detect Access to Restricted Ports

- One label spanning the RJ-45 and mini-USB serial ports, as shown in figure 12. Press down on this label to ensure that it adheres to a sufficient area of the front bezel. The RJ-45 port is raised relative to the bezel so there will be some air gap under the label in this area. However, the air gap should not be larger than 2-3mm.



Figure 11 Required TELs for the Aruba 7008 Mobility Controller – Bottom

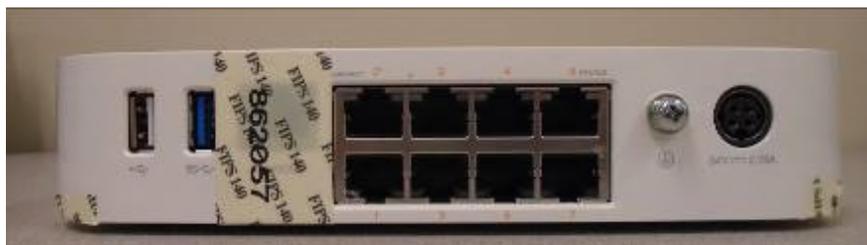


Figure 12 Required TELs for the Aruba 7008 Mobility Controller – Front

The Aruba 7010 Mobility Controller requires a minimum of 6 TELs to be applied as follows:

To Detect Opening the Chassis Lid Top

- Spanning the front bezel and the chassis lid, as shown in Figure 13 (Label 1).

To Detect Opening the Chassis Lid Bottom

- Spanning the bottom and the chassis lid, as shown in Figures 14 and 15 (Labels 3, 4, 5 and 6).

To Detect Access to Restricted Ports

- One label (label 2) spanning the RJ-45 and mini-USB serial ports, as shown in Figure 14. Press down on this label to ensure that it adheres to a sufficient area of the front bezel. The RJ-45 port is raised relative to the bezel so there will be some air gap under the label in this area. However, the air gap should not be larger than 2-3mm.

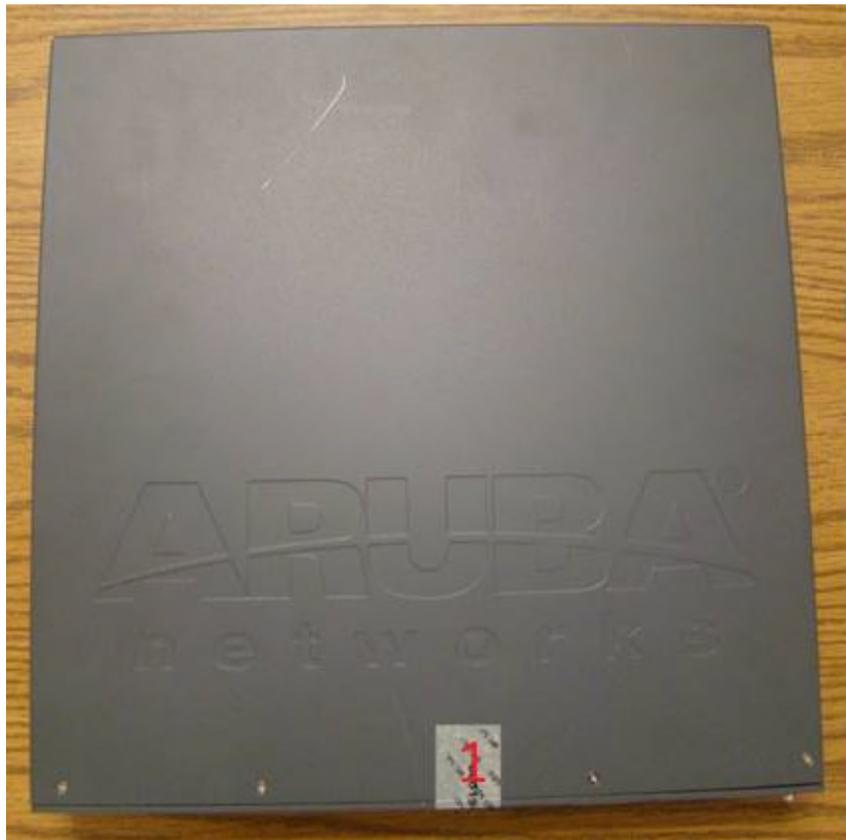


Figure 13 Required TELs for the Aruba 7010 Mobility Controller – Top



Figure 14 Required TELs for the Aruba 7010 Mobility Controller – Front



Figure 15 Required TELs for the Aruba 7010 Mobility Controller – Bottom

The Aruba 7024 Mobility Controller requires a minimum of 7 TELs to be applied as follows:

To Detect Opening the Chassis Lid Top

- Spanning the front bezel and the chassis lid, as shown in Figures 16 and 17 (Label 1).

To Detect Opening the Chassis Lid Bottom

- Spanning the bottom and the chassis lid, as shown in Figure 18 and 19 (Labels 4, 5, 6 and 7).

To Detect Access to Restricted Ports

- One label (label 3) spanning the RJ-45 serial port and one spanning the mini-USB port (label 2) as shown in Figure 16 and 18 (labels 2 & 3). Press down on this label to ensure that it adheres to a sufficient area of the front bezel. The RJ-45 port is raised relative to the bezel so there will be some air gap under the label in this area. However, the air gap should not be larger than 2-3mm.



Figure 16 Required TELs for the Aruba 7024 Mobility Controller - Front



Figure 17 Required TELs for the Aruba 7024 Mobility Controller – Top



Figure 18 Required TELs for the Aruba 7024 Mobility Controller – Rear

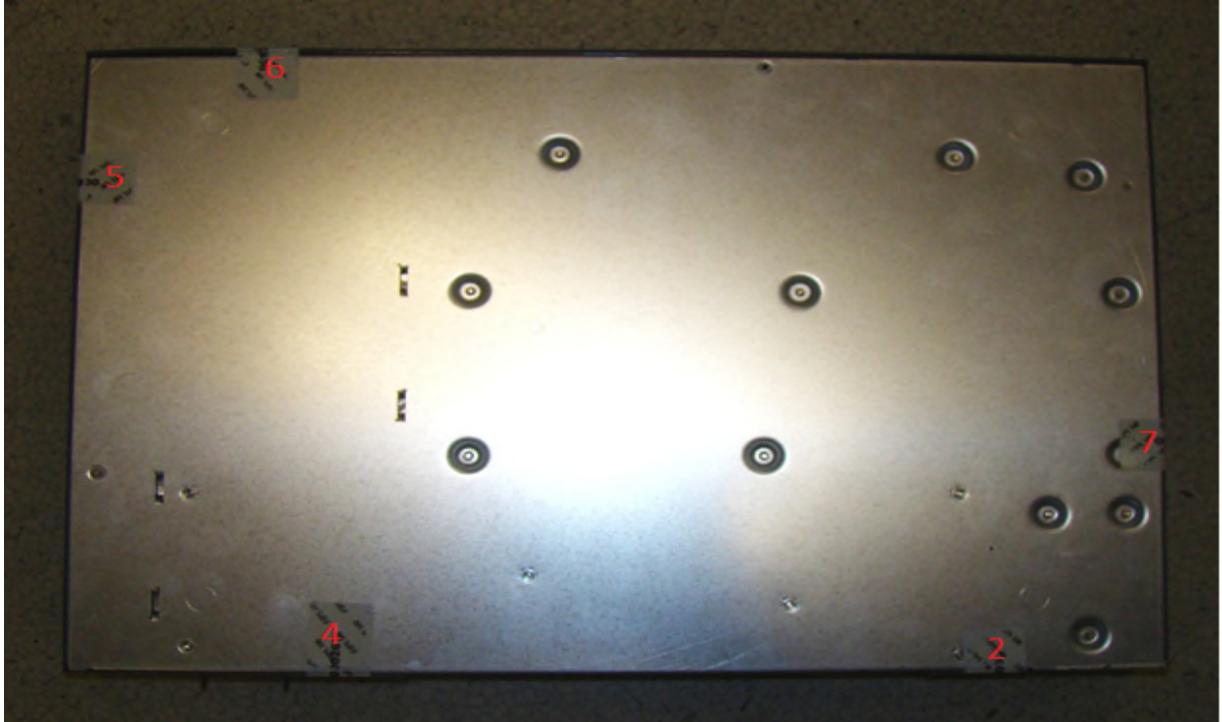


Figure 19 Required TELs for the Aruba 7024 Mobility Controller – Bottom

The Aruba 7030 Mobility Controller requires a minimum of 6 TELs to be applied as follows:

To Detect Opening the Chassis Lid Top

- Spanning the front bezel and the chassis lid, as shown in Figures 20 & 21 (Label 1).

To Detect Opening the Chassis Lid Bottom

- Spanning the bottom and the chassis lid, as shown in Figures 22 (Labels 3, 4, 5 and 6).

To Detect Access to Restricted Ports

- One label (label 2) spanning the RJ-45 and mini-USB serial ports, as shown in figure 21 (Label 2). Press down on this label to ensure that it adheres to a sufficient area of the front bezel. The RJ-45 port is raised relative to the bezel so there will be some air gap under the label in this area. However, the air gap should not be larger than 2-3mm.

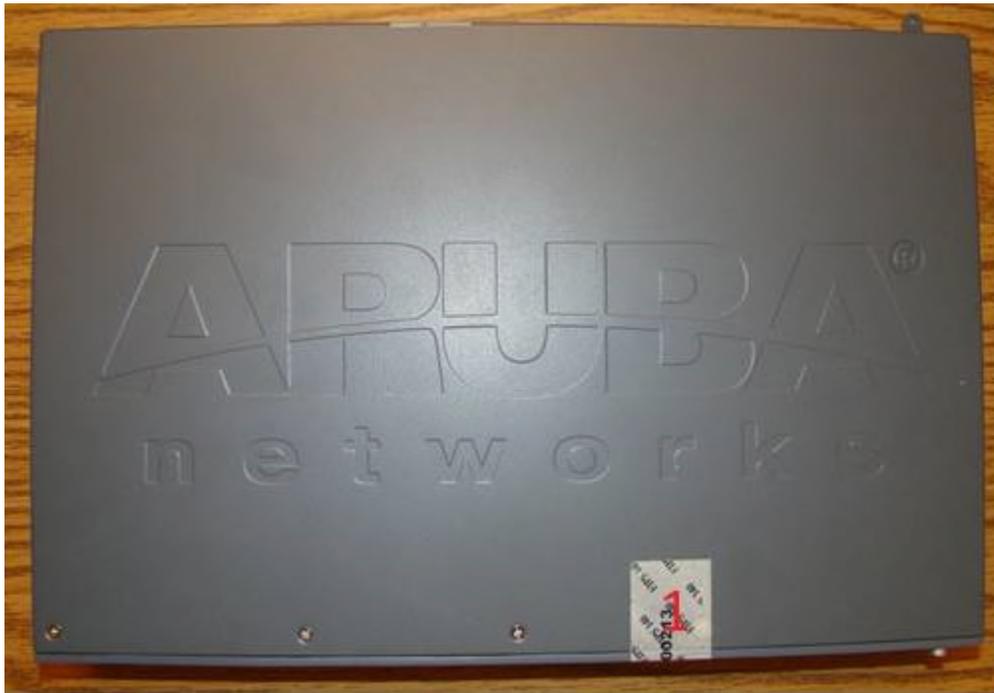


Figure 20 Required TELs for the Aruba 7030 Mobility Controller – Top



Figure 21 Required TELs for the Aruba 7030 Mobility Controller – Front

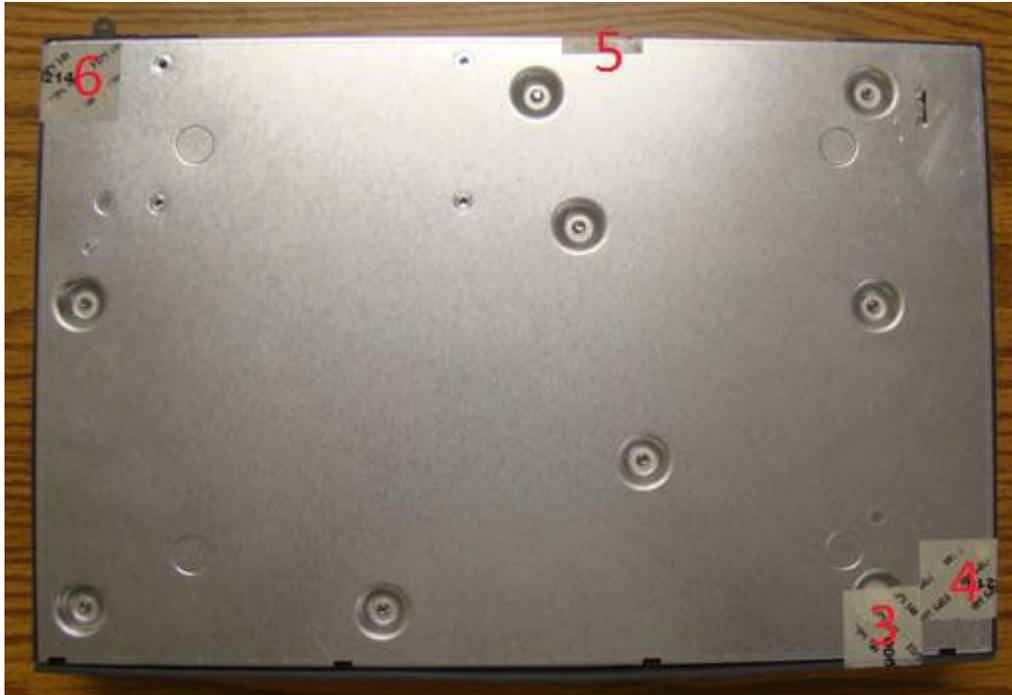


Figure 22 Required TELs for the Aruba 7030 Mobility Controller – Bottom

The Aruba 7205 Mobility Controller requires a minimum of 6 TELs to be applied as follows:

To Detect Opening the Chassis Lid Top

- Spanning the front bezel and the chassis lid, as shown in Figure 23 (Label 1).

To Detect Opening the Chassis Lid Bottom

- Spanning the bottom and the chassis lid, as shown in Figures 24 and 25 (Labels 3, 4, 5 and 6).

To Detect Access to Restricted Ports

- One label (label 2) spanning the RJ-45 and mini-USB serial ports, as shown in Figure 24 (label 2). Press down on this label to ensure that it adheres to a sufficient area of the front bezel. The RJ-45 port is raised relative to the bezel so there will be some air gap under the label in this area. However, the air gap should not be larger than 2-3mm.

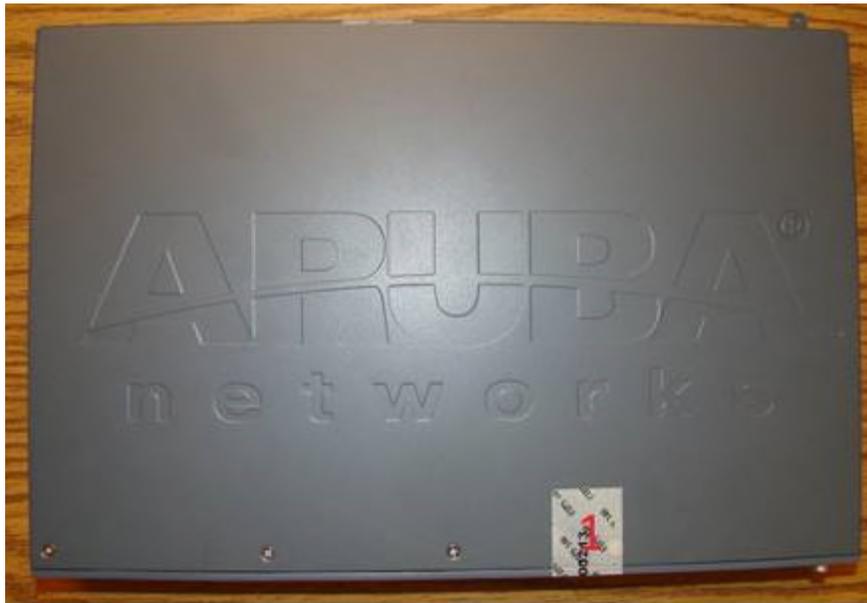


Figure 23 Required TELs for the Aruba 7205 Mobility Controller – Top



Figure 24 Required TELs for the Aruba 7205 Mobility Controller – Front



Figure 25 Required TELs for the Aruba 7205 Mobility Controller – Bottom

The Aruba 7200 (including the 7210, 7220, and 7240 which use the same chassis) Mobility Controller requires a minimum of 15 TELs to be applied as follows:

To Detect Opening the Chassis Lid

- Spanning the left side and right side of the chassis lid where it meets the chassis bottom, as shown in Figures 26, 29, and 30.
- Spanning the front bezel and the chassis lid, as shown in Figures 27 and 28.
- Spanning the expansion slot cover plate and the top of the chassis, as shown in Figures 27 and 28.

To Detect the Removal of Any Module or Cover Plate

- Spanning power supply 1 and the top of the chassis, as shown in Figures 28. If a second power supply is installed, a TEL should be applied to it in an identical way to power supply 1.
- Spanning power supply 2 (if installed) and the top of the chassis, or spanning the power supply 2 cover plate and the top and bottom of the chassis, as shown in Figures 26, 30, and 31.
- Spanning the fan tray and the top and bottom of the chassis, as shown in Figures 26, 27, and 28.

To Detect Access to Restricted Ports

- Two labels spanning the RJ-45 and mini-USB serial ports, as shown in figure 27. Press down on this label to ensure that it adheres to a sufficient area of the front bezel. The RJ-45 port is raised relative to the bezel so there will be some air gap under the label in this area. However, the air gap should not be larger than 2-3mm.



Figure 26 Required TELs for the Aruba 7200 Mobility Controller – Top



Figure 27 Required TELs for the Aruba 7200 Mobility Controller – Front



Figure 28 Required TELs for the Aruba 7200 Mobility Controller – Rear

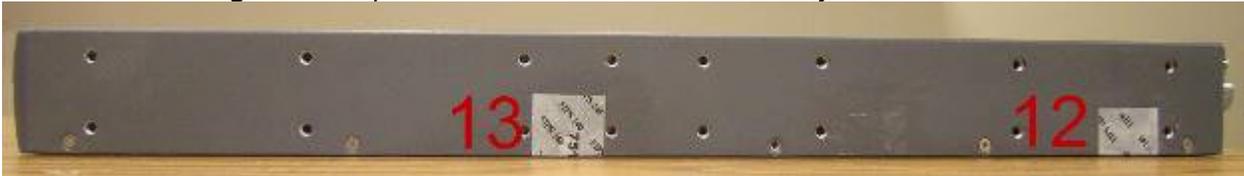


Figure 29 Required TELs for the Aruba 7200 Mobility Controller – Right Side



Figure 30 Required TELs for the Aruba 7200 Mobility Controller – Left Side

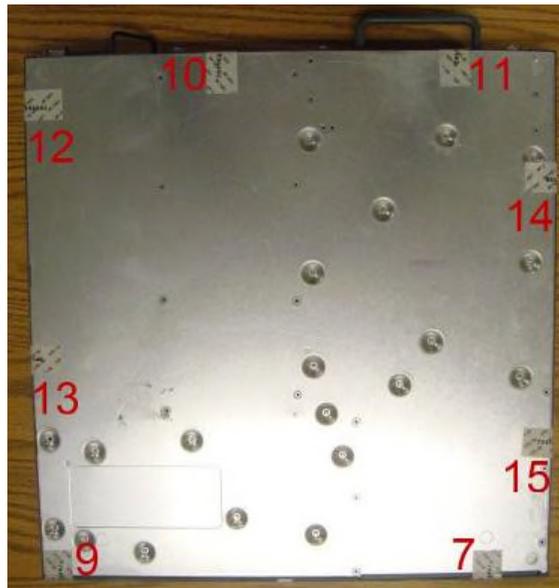


Figure 31 Required TELs for the Aruba 7200 Mobility Controller – Bottom

11.3. Applying TELs

The Crypto Officer should employ TELs as follows:

- Before applying a TEL, make sure the target surfaces are clean and dry. Clean with alcohol and let dry.
- Do not cut, trim, punch, or otherwise alter the TEL.
- Apply the wholly intact TEL firmly and completely to the target surfaces.
- Press down firmly across the entire label surface, making several back-and-forth passes to ensure that the label securely adheres to the chassis.
- Ensure that TEL placement is not defeated by simultaneous removal of multiple modules.
- Allow 24 hours for the TEL adhesive seal to completely cure.
- Record the position and serial number of each applied TEL in a security log.

Once the TELs are applied, the Crypto Officer (CO) should perform initial setup and configuration as described in the next chapter.

11.4. Inspection/Testing of Physical Security Mechanisms

Table 11 - Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanism	Recommended Test Frequency	Guidance
Tamper-evident labels (TELS)	Once per month	Examine for any sign of removal, replacement, tearing, etc. See images above for locations of TELS. If any TELS are found to be missing or damaged, contact a system administrator immediately
Opaque module enclosure	Once per month	Examine module enclosure for any evidence of new openings or other access to the module internals. If any TELS are found to be missing or damaged, contact a system administrator immediately

12. Ongoing Management

The Aruba 7XXX Controllers meet FIPS 140-2 Level 2 requirements. The information below describes how to keep the controller in FIPS-approved mode of operation. The Crypto Officer must ensure that the controller is kept in a FIPS-approved mode of operation.

12.1. Crypto Officer Management

The Crypto Officer must ensure that the controller is always operating in a FIPS-approved mode of operation. This can be achieved by ensuring the following:

- FIPS mode must be enabled on the controller before Users are permitted to use the controller (see “Enabling FIPS Mode”)
- The admin role must be root.
- Passwords must be at least eight characters long.
- VPN services can only be provided by IPsec or L2TP over IPsec.
- Access to the controller Web Interface is permitted only using HTTP over a TLS tunnel. Basic HTTP and HTTP over SSL are not permitted.
- Only SNMP read-only may be enabled.
- Only FIPS-Approved algorithms can be used for cryptographic services. Please refer to section 7.1 for the list of Approved algorithms.
- TFTP can only be used to load backup and restore files. These files are: Configuration files (system setup configuration), the WMS database (radio network configuration), and log files. (FTP and TFTP over IPsec can be used to transfer configuration files.)
- The controller logs must be monitored. If a strange activity is found, the Crypto Officer should take the controller off line and investigate.
- The Tamper-Evident Labels (TEs) must be regularly examined for signs of tampering.
- When installing expansion or replacement modules for the Aruba 7XXX controllers, use only FIPS-approved modules, replace TEs affected by the change, and record the reason for the change, along with the new TE locations and serial numbers, in the security log.
- All configuration performed through the Mobility Master when configured as a managed device must ensure that only the approved algorithms and services are enabled on the FIPS-enabled controller.
- Refer to Section 13.4 for Disallowed Configurations
- The user is responsible for zeroizing all CSPs when switching modes.

13. User Guidance

The User accesses the controller VPN functionality as an IPsec client. The user can also access the controller 802.11i functionality as an 802.11 client. Although outside the boundary of the controller, the User should be directed to be careful not to provide authentication information and session keys to others parties.

13.1. Setup and Configuration

The Aruba 7XXX Controllers meet FIPS 140-2 Level 2 requirements. The sections below describe how to place and keep the controller in FIPS-approved mode of operation. The Crypto Officer (CO) must ensure that the controller is kept in a FIPS-approved mode of operation.

The controller can operate in two modes: the FIPS-approved mode, and the standard non-FIPS mode. By default, the controller operates in non-FIPS mode.

13.2. Setting Up Your Controller

To set up your controller:

1. Make sure that the controller is not connected to any device on your network.
2. Boot up the controller.
3. Connect your PC or workstation to a line port on the controller.

For further details, see the *ArubaOS 8.5.0.0 Getting Started Guide*.

When running as a managed device:

1. Make sure that the controller is connected only to the Mobility Master on your network.
2. Boot up the controller.
3. Connect to the Mobility Master.
4. Follow the procedures as discussed in the *ArubaOS 8.5.0.0 Getting Started Guide*.

13.3. Enabling FIPS Mode

For FIPS compliance, users cannot be allowed to access the controller until the CO changes the mode of operation to FIPS mode. There is one way to enable FIPS mode:

- Use the CLI via SSHv2

13.3.1. Enabling FIPS Mode with the CLI

Login to the controller using an SSHv2 client. Enable FIPS mode using the following commands:

```
#configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(config) #fips enable
(config) #exit
#write memory
Saving Configuration...

Configuration Saved.
```

To verify that FIPS mode has been enabled, issue the command “show fips”.

If logging in to the Controller via the Mobility Master, please reference the user guidance on how to access a managed device. Once connected to the managed controller, the above commands will successfully execute. Please abide by Section 12.1 and 13.4

13.3.2. Disabling the LCD

Configuration through the front-panel LCD should be disabled. To disable the LCD screen, use the following CLI commands:

```
(host) #configure terminal
(host) (config) #lcd-menu
(host) (lcd-menu) #disable menu
```

13.4. Disallowed FIPS Mode Configurations

When you enable FIPS mode, the following configuration options are disallowed:

- All WEP features
- WPA
- TKIP mixed mode
- Any combination of DES, MD5, and PPTP
- Firmware images signed with SHA-1
- Enhanced PAPI Security
- Null Encryption
- TLS with Diffie-Hellman Group 2.
- Certificates with less than 112 bits security strength as used with IKEv1, IKEv2, IPSec, TLS/EAP-TLS, SSH, and/or user authentication.
- Telnet
- EAP-TLS Termination
- Diffie-Hellman Group14 with SHA-256.
- IPSec/IKE using Triple-DES

13.5. Full Documentation

Full documentation can be found at the link provided below.

<https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Default.aspx?EntryId=34189>